one or more client computers which can connect to the Internet and at least one of which can respond to challenges issued by said client premises equipment; and

an enforcement module for selectively blocking Internet access to the Internet to client computers not in compliance with said access policy.

46. (Original) The system of claim 45, wherein said client premises equipment includes a router.

47. (Original) The system of claim 45, wherein said access policy is provided at each client computer to be regulated.

48. (Original) The system of claim 45, wherein said enforcement module is provided at said client premises equipment.

49. (Previously presented) The system of claim 45, wherein said at least one client computer which can respond to challenges responds with a particular predefined code indicating noncompliance with said access policy and is blocked from Internet access.

50. (Previously presented) The system of claim 45, wherein a client computer that responds with a particular predefined code indicating compliance with said access policy is permitted Internet access.

51. (Original) The system of claim 45, wherein at least one of the client computer is capable of transmitting an initial message to the client premises equipment before receipt of a challenge, for requesting the client premises equipment to transmit a challenge to that particular client computer.

52. (Original) The system of claim 45, wherein said enforcement module is capable of permitting Internet access by selected client computers and denying access to other client computers.

53. (Original) The system of claim 45, wherein said access policy includes rules that are enforced against selected ones of users, computers, and groups thereof.

54. (Original) The system of claim 53, wherein said enforcement module is capable of determining, based on identification of a particular client computer or group thereof, a specific subset of said access policies filtered for that particular client computer or group thereof.

55. (Original) The system of claim 45, wherein said access policy specifies

applications that are allowed Internet access.

56. (Original) The system of claim 55, wherein said applications are specified by executable name and version number that are acceptable.

57. (Original) The system of claim 55, wherein said access policy specifies types of activities which applications are allowed to perform or restricted from performing.

58. (Original) The system of claim 55, wherein said applications are specified by digital signatures that are acceptable.

59. (Original) The system of claim 58, wherein said digital signatures are computed using a cryptographic hash.

60. (Original) The system of claim 59, wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-1) and MD5 cryptographic hashes.

61. (Original) The system of claim 45, further comprising:

a sandbox server to which client computers that are not in compliance with said access policy are redirected.

62. (Original) The system of claim 61, wherein said sandbox server informs non-compliant client computers that they are not in compliance with said access policy.

63. (Original) The system of claim 62, wherein said client computers client computers may elect to access the Internet after being informed that they are not in compliance with said access policy.

64. (Original) The system of claim 61, wherein:

said enforcement module is capable of redirecting a client computer that is not in compliance with a particular access policy to a particular port on the sandbox server; and

said sandbox server is capable of displaying particular error message pages in response to communications on particular ports.